A B S T R A C T

The present invention relates to a method of access to a service consisting in i) identifying and registering a client (C), ii) authenticating the client to an anonymous certification authority, iii) authenticating the client by producing an anonymous signature and opening and maintaining an anonymous authentication session with a server (Se), and iv) selectively allowing contact between the server (Se) and the anonymous certification authority (ACA) to revoke the anonymity of the client (C) using the signature provided in step iii). The invention also relates to a system for opening and maintaining an authentication session guaranteeing non-repudiation.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

Rec'd PCT/PTO 13 MAY 2005

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

10/534857

(43) Date de la publication internationale
3 juin 2004 (03.06.2004)

PCT

(10) Numéro de publication internationale
WO 2004/047362 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2003/003380

(22) Date de dépôt international :
14 novembre 2003 (14.11.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/14230 14 novembre 2002 (14.11.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **CANARD, Sébastien** [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). **GUILLOTEAU, Stéphane** [FR/FR]; 42, avenue du 6 Juin, F-14000 Caen (FR). **MALVILLE, Eric** [FR/FR]; 4, rue Maréchal Foch, F-14400 Bayeux (FR). **TRAORE, Jacques** [FR/FR]; 23, avenue de la Suisse Normande, F-61100 Saint Georges des Groseillers (FR).

(74) Mandataires : **MARTIN, Jean-Jacques.** etc.; Cabinet Regimbeau, 20 rue de Chazelles, F-75847 Paris Cedex 17 (FR).

(81) État désigné *(national)* : US.

(84) États désignés *(régional)* : brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Publiée :

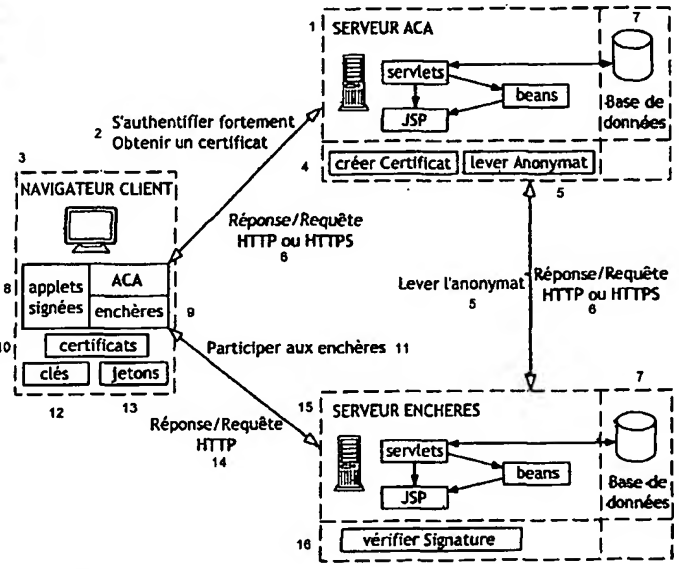
— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM WITH AUTHENTICATION, REVOCABLE ANONYMITY AND NON-REPUDIATION

(54) Titre : PROCEDE ET SYSTEME AVEC AUTHENTIFICATION, ANONYMAT REVOCABLE ET NON REPUDIATION



1 ACA SERVER
2 AUTHENTICATE ONESELF STRONGLY OBTAIN A CERTIFICATE
3 CLIENT BROWSER
4 CREATE CERTIFICATE
5 REMOVE ANONYMITY
6 RESPONSE/REQUEST HTTP OR HTTPS
7 DATABASE
8 SIGNED APPLETS
9 AUCTION
10 CERTIFICATES
11 PARTICIPATE IN AUCTION
12 KEYS
13 TOKENS
14 RESPONSE/REQUEST HTTP
15 AUCTION SERVER
16 VERIFY SIGNATURE

(57) **Abstract:** The invention relates to a method of accessing a service. The inventive method consists in: (i) identifying and registering a Client (C), (ii) authenticating the Client with an Anonymous Certification Authority, (iii) authenticating the Client through the production of an anonymous signature and opening and maintaining an anonymous authentication session with a Server (Se) and (iv) selectively enabling a contact between the Server (Se) and the Anonymous Certification Authority (ACA) in order to remove the anonymity of the Client (C) on the basis of the signature supplied in step (iii). The invention also relates to a system of opening and maintaining an authentication session which guarantees non-repudiation.

(57) **Abrégé :** La présente invention concerne un procédé d'accès à un service consistant à ij identifier et enregistrer un Client (C), ii authentifier le Client auprès d'une Autorité de Certification Anonyme, iii) authentifier le Client par la production d'une signature anonyme et ouvrir et maintenir une session d'authentification anonyme auprès d'un Serveur (Se), etiv permettre sélectivement un contact entre le Serveur (Se) et l'Autorité de Certification Anonyme (ACA) pour lever l'anonymat du Client (C) sur la base de la signature fournie à l'étape iii). L'invention concerne également un système apte à permettre l'ouverture et le maintien d'une session d'authentification garantissant la non répudiation.

WO 2004/047362 A1